UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/506,943	03/07/2005	Carl Gustavsson	9562-9	8802

20792 7590 03/11/2010

MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER	
PHAM, LUU T	
ART UNIT	**PAPER NUMBER**
2437	
MAIL DATE	**DELIVERY MODE**
03/11/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/506,943	GUSTAVSSON ET AL.	
	Examiner	Art Unit	
	LUU PHAM	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 November 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *46-51 and 53-57* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *46-51 and 53-57* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to the Pre-Appeal Brief Request filed on 11/16/2009. Prosecution is hereby re-opened.

2. Claims 1-45, 52, and 58-75 were previously cancelled. Claims 46-51 and 53-57 have been examined and are pending. This Action is made **Non-FINAL**.

Response to Arguments

3. Applicants' arguments with respect to claims 46-51 and 53-57 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

4. **Claim 51 is objected to** because there is a typo in line 3: *"Indentity Module."* It should be *"Identity Module."* Appropriate correction is required.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

7. **Claims 46-49 and 54-56 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Borella et al., (hereinafter "Borella"), U.S. Patent No. 6,353,891, issued on March 5, 2002 and further in view of Matyas, Jr., et al., (hereinafter "Matyas"), U.S. Patent No. 7,010,689, filed on August 21, 2000.

- **Regarding claim 46**, Borella discloses a method for providing authentication when messages are sent between an electronic communication apparatus and a server according to a synchronization protocol in which a plurality of different authentication methods are available *(col. 8, lines 56-67 to col. 9, lines 6-46; Fig. 3)*, comprising:

providing an authentication method indicator that specifies an authentication method of the plurality of different authentication methods according to which the authentication is to be executed *(col. 8, lines 56-67 to col. 9, lines 1-9; Fig. 3; message 1a includes security method parameter 36: 'Security[Method=PSK, Auth=MD5], Security[Method=PSK, Auth=SHA-1]'; security method parameters 36 indicating that the*

client supports the section key method (i.e., PSK), with the appropriate HMAC 34 type (e.g., MD5 and/or SHA-1); see also col. 10, lines 40-49; Fig. 5; message 1a');

incorporating into a message the authentication method indicator comprising a plurality of authentication capabilities of the communication apparatus among the plurality of different authentication methods *(col. 8, lines 56-67 to col. 9, lines 1-9; Fig. 3; message 1a includes security method parameter 36: 'Security[Method=PSK, Auth=MD5], Security[Method=PSK, Auth=SHA-1]'; see also col. 10, lines 40-49; Fig. 5; message 1a')*;

transmitting said message to said server according to an authentication protocol of the synchronization protocol *(col. 8, lines 56-67 to col. 9, lines 1-9; Fig. 3; host device sends message 1a to RSIP gateway; see also col. 10, lines 40-49; Fig. 5; message 1a')*;

generating, at the server, an integrity key an authentication data value *(col. 9, lines 6-23; Fig. 3; RSIP gateway generates response message 1b and sends to host device; response message 1b includes negotiated parameters: userID 31, gateway cookie 38, security method parameter 36 indicating that the session will use the session key method (i.e., PSK), replay counter 33, HMAC 34)* comprising an equivalent of an AKA FRESH parameter *(col. 9, lines 6-23; Fig. 3; wherein at least replay counter 33 and randomly gateway cookie 38; see also col. 9, lines 31-46; col. 10, lines 56-67 to col. 11, lines 1-9)*;

sending the integrity key and the authentication data value to the electronic communication apparatus *(col. 8, lines 32-40; userID and the session key are sent to the host device; col. 9, lines 9-23; Fig. 3; RSIP gateway sends host device response message that includes security parameters 31, 33-34, and 36-38)*;

using the integrity key at the electronic communication apparatus to generate MAC values *(col. 6, lines 65-67 to col. 7, lines 1-4; the value of the HMAC payload's value field may include a hashed message authentication code computed over the entire payload and keyed with a session key)*; and

using a hashing function at the electronic communication apparatus to compute a Hashed Method Authentication Code (HMAC) on the message *(col. 6, lines 65-67 to col. 7, lines 1-4; the value of the HMAC payload's value field may include a hashed message authentication code computed over the entire payload and keyed with a session key)*,

Borella does not explicitly disclose the integrity key is encrypted with the public key of the electronic communication apparatus.

However, in an analogous art, Matyas discloses a secure data storage and retrieval in a client-server environment including steps of generating, at the server, an integrity key that is encrypted with the public key of the electronic communication apparatus *(col. 3, lines 23-29; col. 9, lines 30-52; Figs. 4-5; an integrity key is generated and encrypted using a public key)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Matyas with the system and method of Borella wherein the integrity key is encrypted with the public key of the electronic communication apparatus to provide users with an integrity key and a verification value for secure storage and retrieval of data in a client-server environment *(Matyas: abstract and col. 3, lines 23-29)*.

Borella and Matyas disclose all limitations as recited above, but do not explicitly disclose the specified authentication method is any of a group comprising Wireless Public Key Identity (WPKI), Wireless Identity Module (WIM) authentication.

However, in an analogous art, Lahteenmaki discloses a method for managing network service access and enrolment, wherein the authentication method is WPKI or WIM authentication *(Lahteenmaki: pars. 0038 and 0055; WAP Public key Infrastructure (WPKI) provides a manner of enabling the trust relationships needed for authentication of servers and clients; WIM card manufacturer certificate)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Lahteenmaki with the system and method of Borella and Matyas wherein the authentication method is WPKI or WIM authentication to provide users with a means for managing user access and enrollment for secure network services *(Lahteenmaki: par. 0001)*.

- **Regarding claim 47**, Borella, Matyas, and Lahteenmaki disclose the method according to claim 46.

Borella further discloses the authentication method indicator is incorporated into a meta command of the synchronization protocol *(Borella: col. 8, lines 56-67 to col. 9, lines 1-46; Figs. 3-4; steps 120 and 140; the gateway receives message 1a including negotiated parameters offered by the host device; the host device receives message 1b and records the negotiated parameters in Step 140)*.

- **Regarding claim 48**, Borella, Matyas, and Lahteenmaki disclose the method according to claim 46.

Borella further discloses the message is an initialization message, and the authentication capabilities of the electronic communication apparatus is indicated in an authentication method list of the initialization message, which is sent to the server for establishing a connection *(Borella: col. 8, lines 56-67 to col. 9, lines 1-46; Figs. 3-4; message 1a; REGISTRATION_REQUEST message is known as initialization message; see also col. 10, lines 40-49; Fig. 5; message 1a').*

- **Regarding claim 49**, Borella, Matyas, and Lahteenmaki disclose discloses the method according to claim 46.

Borella further discloses any authentication data relating to the specified authentication method is incorporated in a data string of the message sent according to the synchronization protocol *(Borella: col. 8, lines 56-67 to col. 9, lines 1-46; Fig. 3; message 1a includes security method parameter 36: 'Security[Method=PSK, Auth=MD5], Security[Method=PSK, Auth=SHA-1]').*

- **Regarding claim 54**, Borella, Matyas, and Lahteenmaki disclose discloses the method according to claim 48, further comprising:

Borella further discloses determining at the server the authentication capabilities of the electronic communication apparatus based on the plurality of authentication capabilities listed in the authentication method list *(col. 8, lines 56-67 to col. 9, lines 1-9; Fig. 3; message 1a includes security method parameter 36: 'Security[Method=PSK,*

Auth=MD5], Security[Method=PSK, Auth=SHA-1]'; see also col. 10, lines 40-49; Fig. 5; message 1a'; SHA-1 and MD5 authentications are supported by the client device).

- **Regarding claim 55**, Borella, Matyas, and Lahteenmaki disclose discloses the method according to claim 54.

Borella further discloses executing at the server authentication operations according to one of the plurality of authentication capabilities indicated in the authentication method list *(Borella: col. 9, lines 6-46; col. 10, lines 32-67;)*;

preparing a message at the server comprising the authentication method indicator and any authentication data relating to the specified authentication method *(Borella: col. 9, lines 6-46; col. 10, lines 32-67; the gateway sends REGISTRATION_RESPONSE message 1b containing negotiated parameters (security method parameter 36 indicating that this session will use the session key method (i.e., PSK), and choosing a particular HMAC 34 type (e.g., either MD5 or SHA-1))*; and

transmitting the message to the electronic communication apparatus *(Borella: col. 9, lines 6-46; col. 10, lines 32-67; Fig. 3; REGISTRATION_RESPONSE message 1b containing negotiated parameters is sent to the host device).*

- **Regarding claim 56**, Borella, Matyas, and Lahteenmaki disclose discloses the method according to claim 55.

Borella further discloses receiving the message at the electronic communication apparatus *(Borella: col. 9, lines 6-46; col. 10, lines 32-67; Figs. 3-4; step 140; host device receives message 1b)*;

executing, at the electronic communication apparatus, authentication operations according to the authentication method indicated by the authentication method indicator to generate an expected result *(Borella: col. 9, lines 24-46; Figs. 3-4; steps 140: 'host device receives register_response and records negotiated parameters' and 150: 'host device sends assign_request to RSIP gateway using negotiated parameters'; message 2a)*;

preparing a response to the server comprising the authentication method indicator, and any authentication data *(Borella: col. 9, lines 24-46; Figs. 3-4; step 150; message 2a; host device sends message 2a using the negotiated parameters to RSIP gateway; message 2a includes gateway cookie 38, replay counter 33, and HMAC 34 using Security[Method=PSK, Auth=SHA-1] as selected by the gateway)*; and

transmitting the response to the server *(Borella: col. 9, lines 24-46; Figs. 3-4; step 150; message 2a; host device sends message 2a using the negotiated parameters to RSIP gateway)*.

8. **Claims 50-51 and 57 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Borella, Matyas, and Lahteenmaki, as applied to claim 46 above, and further in view of Quick, Jr. et al., (hereinafter "Quick"), U.S. Patent Application No. 2002/0091933, filed on May 22, 2001.

- **Regarding claim 50**, Borella, Matyas, and Lahteenmaki disclose discloses the method according to claim 46.

Borella, Matyas, and Lahteenmaki do not explicitly disclose the authentication method is Global System for Mobile communications (GSM) Subscriber Identity Module (SIM) authentication.

However, in an analogous art, Quick discloses a method for providing local authentication, wherein the authentication method is Global System for Mobile communications (GSM) Subscriber Identity Module (SIM) authentication *(Quick: pars. 0005-0006; Subscriber Identity Module (SIM) is used in GSM system; an authentication key for identifying the subscriber).*

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Quick with the system and method of Borella, Matyas, and Lahteenmaki, wherein authentication method is Global System for Mobile communications (GSM) Subscriber Identity Module (SIM) authentication to provide users with a mean for providing secure authentication to a subscriber roaming outside his or her home system *(Quick: par. 0007).*

- **Regarding claim 51**, Borella, Matyas, and Lahteenmaki disclose discloses the method according to claim 46.

Borella, Matyas, and Lahteenmaki do not explicitly disclose the authentication method is Universal Mobile telephone System (UMTS) Universal Subscriber Indentity Module (USIM) authentication, which provides server authentication.

However, in an analogous art, Quick discloses a method for providing local authentication, wherein the authentication method is Universal Mobile telephone System (UMTS) Universal Subscriber Indentity Module (USIM) authentication, which provides

server authentication *(Quick: pars. 0005 and 0006; next generation SIM card have been renamed as USIM used in UTMS system; an authentication key for identifying the subscriber)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Quick with the system and method of Borella, Matyas, and Lahteenmaki, wherein the authentication method is Universal Mobile telephone System (UMTS) Universal Subscriber Indentity Module (USIM) authentication, which provides server authentication to provide users with a mean for providing secure authentication to a subscriber roaming outside his or her home system *(Quick: par. 0007)*.

- **Regarding claim 57**, Borella, Matyas, and Lahteenmaki disclose discloses the method according to claim 46.

Borella and Matyas further disclose using CKs/IKs (cipher keys/integrity keys) generated by the electronic communication apparatus and the server, respectively, to provide integrity protection, wherein the CKs/IKs are used for generating MAC values *(Borella: col. 6, lines 65-67 to col. 7, lines 1-4; the value of the HMAC payload's value field may include a hashed message authentication code computed over the entire payload and keyed with a session key; Matyas: col. 9, lines 36-39; col. 9, lines 58-65; Fig. 5; wherein at least step 512-524; HMAC is generated integrity key Ki and SHA-1 algorithm)*; and

using a hashing function for computing a Hashed Method Authentication Code (HMAC) on the message *(Borella: col. 6, lines 65-67 to col. 7, lines 1-4; the value of the*

HMAC payload's value field may include a hashed message authentication code computed over the entire payload and keyed with a session key; Matyas: col. 9, lines 36-39; col. 9, lines 58-65; Fig. 5; wherein at least step 512-524; HMAC is generated integrity key Ki and SHA-1 algorithm).

Borella, Matyas, and Lahteenmaki do not explicitly disclose the authentication method is Subscriber Identity Module/Universal Subscriber Identity Module (SIM/USIM) authentication.

However, in an analogous art, Quick discloses a method for providing local authentication, wherein the authentication method is Subscriber Identity Module/Universal Subscriber Identity Module (SIM/USIM) authentication *(Quick: pars. 0005 and 0006; next generation SIM card have been renamed as USIM used in UTMS system; an authentication key for identifying the subscriber).*

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Quick with the system and method of Borella, Matyas, and Lahteenmaki, wherein the authentication method is Subscriber Identity Module/Universal Subscriber Identity Module (SIM/USIM) authentication to provide users with a mean for providing secure authentication to a subscriber roaming outside his or her home system *(Quick: par. 0007).*

9. **Claim 53 is rejected under 35 U.S.C. 103(a)** as being unpatentable over Borella, Matyas, and Lahteenmaki, as applied to claim 46 above, and further in view of Tran et al., (hereinafter "Tran"), U.S. Patent Application No. 2003/0033524, filed on August 13, 2001.

- **Regarding claim 53**, Borella, Matyas, and Lahteenmaki disclose the method according to claim 46.

Borella, Matyas, and Lahteenmaki do not explicitly disclose the authentication method is SecureId or SafeWord authentication.

However, in an analogous art, Tran discloses a wireless portal system, wherein the authentication method is SecureId or SafeWord authentication *(Tran: par. 0052; the authentication modules may also include LDAP authentication, secure ID, radius authentication, etc.)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Tran with the method of Borella, Matyas, and Lahteenmaki wherein the authentication method is SecureId or SafeWord authentication to provide access to any type of service from any type of device from anywhere and to provide content suitable for these devices without incurring substantial cost overhead *(Tran: par. 0008)*.

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Luu Pham whose telephone number is 571-270-5002. The examiner can normally be reached on Monday through Friday, 7:30 AM - 5:00 PM (EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Luu Pham/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437